

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1-65. (Canceled).

66. (Currently Amended) A computing device for communicating with a remotely located computing device, the computing device comprising:

a non-transitory computer-readable medium or media encoded with instructions to allow the computing device to perform the following tasks:

transmitting upon an occurrence of a predetermined event, from the computing device to the remotely located computing device, a lock session signal for locking a communications session upon the occurrence of the predetermined event, the lock session signal configured to restrict access to the communications session until the computing device receives an unlock session signal from the remotely located computing device;

prompting a user at the computing device for identification information associated with the communications session;

transmitting, from the computing device to the remotely located computing device, the identification information; and

receiving, at the computing device from the remotely located computing device, the unlock session signal if the identification information is authenticated,

wherein the predetermined event comprises a detection of a departure of the user without manual input from the user,

wherein the computing device is configured to facilitate communication of the communications session using a first communication channel, and is configured to facilitate communication of the lock session signal, the unlock session signal, and the identification information using a second communication channel, and

wherein communications occurring through the first communication channel are suspended when the communications session is locked.

67. (Canceled)

68. (Currently Amended) The computing device of Claim [[67]] 66, wherein the second communication channel is a Citrix® Independent Computing Architecture™ (ICA) Virtual Channel.

69. (Canceled)

70. (Previously Presented) The computing device of Claim 66, wherein the predetermined event further comprises a lapse in a predetermined amount of time.

71. (Previously Presented) The computing device of Claim 66, wherein the predetermined event further comprises an activation of a screen saver.

72. (Previously Presented) The computing device of Claim 66, wherein the computing device is a personal computer.

73. (Previously Presented) The computing device of Claim 66, wherein the computing device is an automated teller machine (ATM).

74. (Previously Presented) The computing device of Claim 66, wherein the computing device is an industrial controller.

75. (Previously Presented) The computing device of Claim 66, wherein the computing device is a gateway.

76. (Previously Presented) The computing device of Claim 66, wherein the computing device is an internet protocol (IP) telephone.

77. (Previously Presented) The computing device of Claim 66, wherein the computing device is a thin client.

78. (Previously Presented) The computing device of Claim 66, wherein the computing device is a personal digital assistant (PDA).

79. (Previously Presented) The computing device of Claim 66, wherein the computing device is a cellular telephone.

80. (Previously Presented) The computing device of Claim 66, wherein the identification information is not a shared screen saver password.

81. (Previously Presented) The computing device of Claim 66, wherein the computing device is configured to allow a session management operation to be triggered locally using an application at the computing device, but executed at the remotely located computing device.

82. (Previously Presented) The computing device of Claim 66, wherein the transmitting the lock session signal for the communications session comprises transmitting the lock session signal to lock the communications session at the remotely located computing device.

83. (Previously Presented) The computing device of Claim 66, wherein the computing device is configured to facilitate a local lock at the computing device and a session lock at the remotely located computing device.

84. (Currently Amended) A non-transitory computer-readable medium or media encoded with instructions for facilitating management of a communications session, the instructions comprising code for:

transmitting upon an occurrence of a predetermined event, from a computing device to a remotely located computing device, a lock session signal for locking a communications session upon the occurrence of the predetermined event, the lock session signal configured to restrict access to the communications session until the computing device receives an unlock session signal from the remotely located computing device;

prompting a user at the computing device for identification information associated with the communications session;

transmitting, from the computing device to the remotely located computing device, the identification information; and

receiving, at the computing device from the remotely located computing device, the unlock session signal if the identification information is authenticated,

wherein the predetermined event comprises a detection of a departure of the user without manual input from the user,

wherein the computing device is configured to facilitate communication of the communications session using a first communication channel, and is configured to facilitate communication of the lock session signal, the unlock session signal, and the identification information using a second communication channel, and

wherein communications occurring through the first communication channel are suspended when the communications session is locked.

85. (Currently Amended) A method for facilitating management of a communications session from a client computing device, comprising the steps of:

transmitting upon an occurrence of a predetermined event, from the client computing device to a remotely located computing device, a lock session signal for locking a communications session upon the occurrence of the predetermined event, the lock session signal configured to restrict access to the communications session until the client computing device receives an unlock session signal from the remotely located computing device;

prompting a user at the client computing device for identification information associated with the communications session;

transmitting, from the client computing device to the remotely located computing device, the identification information; and

receiving, at the client computing device from the remotely located computing device, the unlock session signal if the identification information is authenticated,

wherein the predetermined event comprises a detection of a departure of the user without manual input from the user,

wherein the client computing device is configured to facilitate communication of the communications session using a first communication channel, and is configured to facilitate communication of the lock session signal, the unlock session signal, and the identification information using a second communication channel, and

wherein communications occurring through the first communication channel are suspended when the communications session is locked.

86. (Previously Presented) The computing device of Claim 66, wherein the detection of the departure of the user without manual input from the user is performed using at least one of the following without manual input by the user indicating the departure: a motion detector, a presence or an absence of a dedicated short range communication identification device, or an altered biometric data of the user.

87. (Previously Presented) The computing device of Claim 66, wherein the tasks further comprise receiving information about the user, and wherein the detection of the departure of the user without manual input from the user is performed by software configured to use artificial intelligence to examine input or writing style of another user.